AI RISK ASSESSMENT DASHBOARD

Project: AI Document Processing System
Assessment Date January 20, 2026
Risk Owner: Project Risk Manager
Last Updated: January 20, 2026

RISK SUMMARY BY LEVEL

Risk Level	Count	Open	Closed
Critical	2	2	0
High	6	4	2
Medium	8	6	2
Low	4	2	2
TOTAL RISKS:	**20**		

RISKS BY CATEGORY

Category	Critical/High	Total
Model Performance	2	3
Data Quality	1	2
Bias/Fairness	2	2
Explainability	1	2
Security	0	1
Privacy	1	3
Operational	0	3
Business	0	1
Reputational	0	1

TOP 5 RISKS REQUIRING IMMEDIATE ATTENTION

Risk ID	Risk Description	Level	Status	Owner
R-002	Training data bias leading to discriminatory out	**Critical**	Open	Ethics Officer
R-001	Model accuracy below 95% threshold	**Critical**	In Progress	Data Science Lead
R-005	GDPR compliance failure	**High**	In Progress	Compliance Lead
R-003	Personal data exposure through model	**High**	In Progress	Privacy Officer
R-004	Inability to explain decisions	**High**	Open	ML Engineer

AI PROJECT RISK REGISTER

Risk ID	Risk Title	Risk Category	Risk Description	Likelihood	Impact	Risk Level	Mitigation Strategy	Specific Actions	Owner	Target Date	Residual Likelihood	Residual Impact	Residual Risk	Status	Notes	Date Identified	Last Updated
R-001	Model Accuracy Below Threshold	Model Performance	AI model fails to meet 95% accuracy threshold required for automated processing. Model performs at only 88% accuracy on validation set.	3	4	High	Mitigate	1) Expand training data to 500K+ documents 2) Implement confidence thresholds - route <95% cases to human review 3) Add model ensemble approach 4) Conduct additional feature engineering	Data Science Lead	2026-03-15	2	3	Medium	In Progress	Training data expansion in progress. Current validation accuracy: 91%	2026-01-05	2026-01-19
R-002	Training Data Bias	Bias/Fairness	Historical training data reflects past discriminatory practices in vendor treatment. Model may perpetuate bias, leading to differential processing speed/accuracy by vendor demographic characteristics.	4	5	Critical	Mitigate	1) Conduct comprehensive fairness assessment across vendor demographics 2) Implement fairness-aware algorithm (demographic parity) 3) Test model performance by vendor groups 4) Create bias monitoring dashboard	Ethics Officer	2026-02-28	2	4	High	Open	Fairness assessment scheduled for Week of Jan 27. External consultant engaged.	2026-01-08	2026-01-19
R-003	Personal Data Exposure	Data Privacy	Invoices contain personal identifiable information (PII) including names, addresses, SSNs. Risk of unauthorized exposure through model inference, logging, or data breaches.	2	5	High	Mitigate	1) Implement data minimization - remove PII before training 2) Use differential privacy techniques in model 3) Encrypt all data at rest and in transit 4) Implement strict access controls 5) Conduct Data Protection Impact Assessment (DPIA)	Privacy Officer	2026-02-15	1	4	Low	In Progress	DPIA completed. PII removal process implemented. Encryption in progress.	2026-01-05	2026-01-18
R-004	Inability to Explain Decisions	Explainability	Deep learning model is black box - cannot explain why specific invoices were approved/rejected. Creates regulatory compliance issues and stakeholder distrust.	4	3	High	Mitigate	1) Implement SHAP (SHapley Additive exPlanations) for model explainability 2) Create decision audit trails 3) Develop user-facing explanation interface 4) Document decision logic and key features 5) Consider switching to more interpretable model for	ML Engineer	2026-03-01	2	2	Medium	Open	SHAP library evaluated. Prototype explanation interface in development.	2026-01-10	2026-01-19
R-005	GDPR Compliance Failure	Regulatory	AI system may violate GDPR requirements for data protection, right to explanation, automated decision-making, and consent management.	2	5	High	Mitigate	1) Engage legal counsel for GDPR assessment 2) Implement data retention and deletion policies 3) Create consent management system 4) Document all data processing purposes 5) Enable data subject rights (access, rectification, erasure)	Compliance Lead	2026-02-28	1	4	Low	In Progress	Legal review in progress. Compliance documentation 70% complete.	2026-01-05	2026-01-17
R-006	User Rejection Due to Poor Change Management	Business	Users resist AI system due to job security fears, lack of trust, or poor training. Results in low adoption, workarounds, and failure to realize benefits.	3	4	High	Mitigate	1) Develop comprehensive change management plan 2) Conduct extensive training (90+ minutes hands-on) 3) Address job security concerns openly and honestly 4) Implement pilot with champions 5) Create feedback loops and act on input 6) Provide ongoing support (help desk, refresher training)	Change Manager	2026-04-01	2	3	Medium	In Progress	Change plan approved. Training curriculum finalized. Pilot team selected.	2026-01-12	2026-01-19
R-007	Model Performance Degradation Over Time	Model Performance	Model accuracy degrades as invoice formats, vendor practices, and document types evolve. Model trained on current data becomes obsolete.	4	3	High	Mitigate	1) Implement continuous accuracy monitoring with automated alerts 2) Set trigger at <97% accuracy for investigation 3) Plan quarterly model retraining schedule 4) Monitor data distribution shifts 5) Create model versioning and rollback procedures	MLOps Lead	2026-03-15	2	2	Medium	Open	Monitoring framework under development. Alert system 50% complete.	2026-01-10	2026-01-19
R-008	ERP Integration Failure	Operational	Integration with legacy ERP system fails, causing data loss, corruption, or processing delays. API compatibility issues or data format mismatches.	2	4	Medium	Mitigate	1) Conduct early integration testing with ERP sandbox 2) Implement transaction rollback capabilities 3) Create comprehensive data validation 4) Build monitoring and alerting for integration points 5) Develop rollback and recovery procedures 6) Maintain parallel manual processing for 30 days	Integration Lead	2026-03-30	1	3	Low	In Progress	Integration testing 60% complete. No major issues identified yet.	2026-01-08	2026-01-18
R-009	Insufficient Training Data Quality	Data Quality	Training data contains errors, inconsistencies, missing values. Historical data may have incorrect labels or outdated information.	3	4	High	Mitigate	1) Conduct comprehensive data quality assessment 2) Implement data cleaning and validation pipeline 3) Create data quality standards and checks 4) Manual review and correction of 10% sample 5) Establish data quality monitoring 6) Improve data collection processes going forward	Data Engineer	2026-02-28	2	3	Medium	In Progress	Data quality assessment 80% complete. 15% error rate identified.	2026-01-05	2026-01-19
R-010	Edge Case Handling Failure	Model Performance	Model fails on rare but important document types or scenarios not well-represented in training data (e.g., foreign invoices, unusual formats, handwritten notes).	4	3	High	Mitigate	1) Identify and document edge cases systematically 2) Augment training data with edge case examples 3) Implement confidence thresholds - route uncertain cases to humans 4) Create escalation procedures for edge cases 5) Build edge case library from production experience	Data Science Lead	2026-03-15	3	2	Medium	Open	Edge case analysis in progress. 23 edge case types identified so far.	2026-01-12	2026-01-19
R-011	Cross-Border Data Transfer Violations	Data Privacy	Processing invoices from EU customers may violate data localization requirements. Data transfer to US-based cloud infrastructure without proper safeguards.	2	4	Medium	Mitigate	1) Implement EU data residency (process EU data in EU datacenter) 2) Execute Standard Contractual Clauses (SCCs) 3) Conduct Transfer Impact Assessment 4) Consider federated learning approach	Privacy Officer	2026-03-15	1	3	Low	Open	EU datacenter deployment planned. SCC review with legal in progress.	2026-01-15	2026-01-19
R-012	Adversarial Attack Vulnerability	Security	Malicious actors could craft invoices specifically designed to fool AI model into incorrect classification or data extraction.	2	3	Medium	Mitigate	1) Conduct adversarial robustness testing 2) Implement input validation and anomaly detection 3) Add rate limiting to prevent systematic probing 4) Monitor for unusual patterns 5) Maintain human oversight for high-value transactions	Security Lead	2026-03-30	1	2	Low	Open	Adversarial testing framework being evaluated. Anomaly detection in scope.	2026-01-14	2026-01-19
R-013	AI Act High-Risk Classification	Regulatory	EU AI Act may classify invoice processing as high-risk AI system, triggering extensive compliance requirements (risk management, documentation, human oversight).	3	3	Medium	Mitigate	1) Conduct AI Act applicability assessment 2) Implement conformity assessment procedures if required 3) Create technical documentation file 4) Establish quality management system 5) Implement logging and transparency requirements	Compliance Lead	2026-04-30	2	2	Medium	Open	Monitoring EU AI Act implementation timeline. Risk classification uncertain.	2026-01-10	2026-01-17
R-014	Insufficient Infrastructure Capacity	Operational	AI system cannot handle production volumes (50K documents/month). GPU compute insufficient, causing processing delays and user frustration.	2	3	Medium	Mitigate	1) Conduct comprehensive load testing at 150% expected volume 2) Design auto-scaling infrastructure 3) Optimize model for inference performance 4) Implement queuing and batch processing 5) Plan capacity buffer (20% above expected peak)	Infrastructure Lead	2026-03-15	1	2	Low	In Progress	Load testing at 100K docs/month successful. Auto-scaling configured.	2026-01-08	2026-01-18

R-015	Vendor Dependency Risk	Operational	Reliance on single cloud AI platform creates vendor lock-in. Platform changes, price increases, or service discontinuation could disrupt operations.	2	3	**Medium**	Transfer/Mitigate	1) Design model to be platform-agnostic where feasible 2) Maintain model artifacts in portable format 3) Document migration procedures 4) Negotiate service level agreements with penalty clauses 5) Budget for potential platform migration	Technical Architect	2026-04-15	2	2	Medium	Open	Architecture review scheduled. Portability strategy in development.	2026-01-12	2026-01-19
R-016	Language Bias in OCR	Bias/Fairness	OCR component performs worse on non-English documents or documents with accented characters, disadvantaging non-native English vendors.	3	3	**Medium**	Mitigate	1) Test OCR across multiple languages and character sets 2) Use multilingual OCR models 3) Monitor accuracy by language 4) Provide alternative submission methods for affected vendors 5) Manual review for low-confidence non-English	Data Science Lead	2026-03-01	2	2	Medium	Open	Language testing plan developed. Multilingual OCR being evaluated.	2026-01-15	2026-01-19
R-017	Data Pipeline Failure	Data Quality	Automated data pipeline feeding training/production data fails due to upstream system changes, causing stale data or processing stoppage.	3	3	**Medium**	Mitigate	1) Implement comprehensive pipeline monitoring 2) Create automated alerts for data freshness 3) Build data quality checks at each pipeline stage 4) Develop fallback data sources 5) Document pipeline dependencies and change management	Data Engineer	2026-02-28	2	2	Medium	In Progress	Monitoring framework 70% complete. Alert system implemented.	2026-01-10	2026-01-18
R-018	Negative Media Coverage of AI Use	Reputational	Public or media backlash against AI automation, especially if job losses or errors become public. "AI replaces workers" narrative damage.	2	3	**Medium**	Mitigate	1) Develop proactive communication strategy emphasizing augmentation not replacement 2) Ensure no job losses attributable to AI 3) Highlight benefits to employees (less tedious work) 4) Create transparency in AI use 5) Prepare crisis communication plan	Communications Lead	2026-03-01	1	2	Low	In Progress	Communication strategy approved. Messaging guidelines distributed.	2026-01-12	2026-01-17
R-019	Audit Trail Inadequacy	Explainability	Insufficient logging of AI decisions makes post-hoc investigation impossible. Cannot reconstruct why specific decision was made.	3	3	**Medium**	Mitigate	1) Implement comprehensive decision logging (inputs, outputs, confidence, timestamp) 2) Log model version and features used 3) Create audit query interface 4) Define retention policy for audit logs 5) Test audit trail completeness	ML Engineer	2026-03-15	1	2	Low	In Progress	Logging framework implemented. Retention policy defined (7 years).	2026-01-14	2026-01-19
R-020	Model Inversion Attack	Data Privacy	Attacker could extract sensitive training data information through systematic querying of model (privacy attack on training data).	1	4	**Low**	Mitigate	1) Implement differential privacy in model training 2) Add rate limiting to prevent systematic probing 3) Monitor for suspicious query patterns 4) Minimize PII in training data 5) Regular privacy vulnerability assessments	Security Lead	2026-03-30	1	3	Low	Open	Differential privacy techniques being evaluated. Low probability but included for completeness.	2026-01-15	2026-01-19

RISK RATING SCALES & CATEGORIES

LIKELIHOOD SCALE (Probability of Occurrence)

Rating	Level	Probability	Description
1	Rare	< 10%	May occur only in exceptional circumstances
2	Unlikely	10-30%	Could occur but not expected
3	Possible	30-50%	Might occur at some point
4	Likely	50-75%	Will probably occur
5	Almost Certain	> 75%	Expected to occur in most circumstances

IMPACT SCALE (Consequences if Risk Occurs)

Rating	Level	Cost/Time	Description
1	Negligible	Minimal	Easily managed with existing resources. No
2	Minor	< 5%	Limited attention required. Minor
3	Moderate	5-15%	Management attention required. Delays
4	Major	15-30%	Threatens project success. Delays of 3-6
5	Severe	> 30%	Critical impact. Delays > 6 months. Severe

RISK LEVEL MATRIX (Likelihood × Impact)

Risk Level Definitions:

CRITICAL (Red)	Immediate action required. May block deployment. Weekly monitoring.
HIGH (Orange)	Urgent attention needed. Escalate to leadership. Bi-weekly monitoring.
MEDIUM (Yellow)	Manage with defined controls. Monthly monitoring.
LOW (Green)	Accept with basic monitoring. Quarterly review.

AI RISK CATEGORIES

Category	Key Risks
Model Performance	Model accuracy, performance degradation, edge cases, overfitting
Data Quality	Data quality, availability, drift, pipeline failures, label quality
Bias/Fairness	Historical bias, representation bias, algorithmic bias, discrimination
Explainability	Black box models, transparency, audit challenges, decision explanations
Security	Adversarial attacks, data poisoning, model theft, privacy attacks
Data Privacy	PII exposure, re-identification, data retention, consent violations
Regulatory	Non-compliance with AI regulations, GDPR, CCPA, industry standards
Operational	Deployment failures, integration issues, scalability, infrastructure
Business	ROI shortfall, adoption failure, change resistance, vendor lock-in
Reputational	Public backlash, customer distrust, ethical violations, stakeholder harm

HOW TO USE THIS RISK REGISTER

OVERVIEW

This AI Risk Register is a comprehensive tool for systematically identifying, assessing, and managing risks specific to AI projects. It includes:

- Risk Dashboard: Executive summary showing risk status at a glance
- Risk Register: Detailed register of all identified risks with ratings and mitigation plans
- Rating Scales: Standardized scales for assessing likelihood, impact, and risk level
- Instructions: This sheet - guidance on using the risk register effectively

The register contains 20 sample risks across all major AI risk categories to serve as a template for your own AI project risk assessment.

HOW TO USE THIS REGISTER

1. Review Sample Risks

Examine the 20 sample risks in the Risk Register sheet. These cover all major AI risk categories and provide realistic examples for an AI document processing project.

2. Customize for Your Project

Replace sample risks with risks specific to your AI initiative. Keep relevant risks, remove those that don't apply, add new risks unique to your context.

3. Assess Each Risk

For each risk, evaluate:

- Likelihood (1-5): Probability of occurrence
- Impact (1-5): Consequences if it occurs
- Risk Level: Automatically determined by Likelihood × Impact using the matrix in Rating Scales sheet

4. Develop Mitigations

For each significant risk, document:

- Mitigation Strategy: Avoid, Mitigate, Transfer, or Accept
- Specific Actions: Concrete steps to address the risk
- Owner: Person responsible for managing the risk

5. Calculate Residual Risk

After mitigations, re-assess:

- Residual Likelihood: Probability after controls
- Residual Impact: Consequences if still occurs
- Residual Risk Level: Is remaining risk acceptable?

6. Monitor and Update

Risks are living - update regularly:

- Review at project milestones
- Track mitigation progress (Status column)
- Re-assess as project evolves

7. Communicate to Stakeholders

Use Dashboard sheet for executive briefings. Use full Register for governance boards and detailed reviews. Color-coded risk levels make priorities immediately visible.

RISK REGISTER FIELD DEFINITIONS

Risk ID	Unique identifier for tracking (e.g., R-001, R-002)
Risk Title	Short, descriptive name for the risk
Risk Category	Category from: Model Performance, Data Quality, Bias/Fairness, Explainability, Security, Privacy, Regulatory, Operational, Business, Reputational
Risk Description	Detailed description of the risk, including potential causes and consequences
Likelihood	Probability of occurrence (1-5 scale - see Rating Scales sheet)
Impact	Severity of consequences if risk occurs (1-5 scale - see Rating Scales sheet)
Risk Level	Overall risk priority: Critical, High, Medium, or Low (based on Likelihood × Impact matrix)
Mitigation Strategy	Approach: Avoid (eliminate risk), Mitigate (reduce likelihood/impact), Transfer (shift to third party), Accept (acknowledge and monitor)
Specific Actions	Concrete steps to implement mitigation strategy
Owner	Person responsible for managing this risk
Target Date	When mitigation actions should be completed
Residual Likelihood	Likelihood after mitigation (1-5 scale)

Residual Impact	Impact after mitigation (1-5 scale)
Residual Risk	Risk level after mitigation - should be acceptable to organization
Status	Current state: Open, In Progress, Closed
Notes	Additional context, progress updates, or relevant information
Date Identified	When this risk was first identified
Last Updated	Most recent update to this risk record

BEST PRACTICES

✓ Start early - conduct initial risk assessment during project conception, not before deployment
✓ Be comprehensive - use all 9 AI risk categories to ensure thorough identification
✓ Involve diverse perspectives - include technical, business, legal, ethics, and security experts
✓ Document thoroughly - future audits and retrospectives require detailed records
✓ Be specific - vague risks lead to vague mitigations; make everything actionable
✓ Prioritize ruthlessly - focus mitigation efforts on Critical and High risks
✓ Monitor continuously - risks evolve as projects progress; review at each milestone
✓ Close the loop - track mitigations to completion and validate effectiveness
✓ Communicate transparently - honest risk communication builds stakeholder trust
✓ Learn from experience - update risk catalog based on what actually materializes